BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/060121 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/US01/43736

(22) International Filing Date:
19 November 2001 (19.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/752,974 27 December 2000 (27.12.2000) US

(71) Applicant *(for all designated States except US)*: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GRAWROCK, David, W.** [US/US]; 8285 Southwest 184th Avenue, Aloha, OR 97007 (US).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely Sokoloff Tayolor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

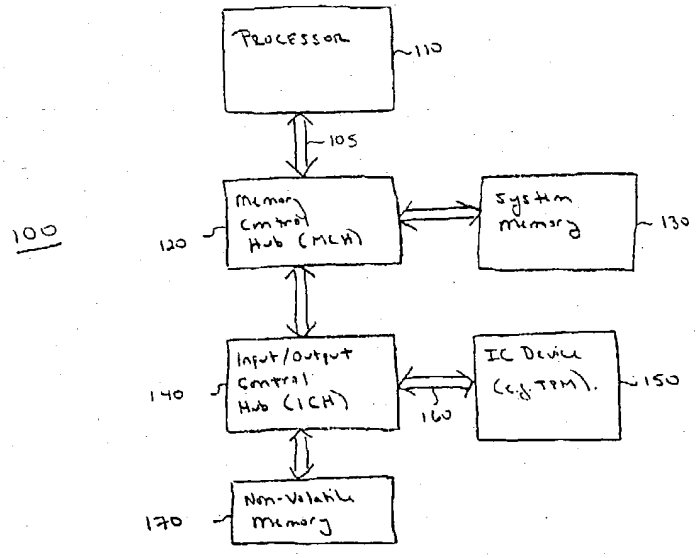
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A PLATFORM AND METHOD FOR SECURELY TRANSMITTING AUTHORIZATION DATA



(57) Abstract: In one embodiment, a platform comprises a processor, an input/output control hub (ICH), and a trusted platform module (TPM). Coupled to the ICH, the TPM comprises an internal memory, and an asymmetric key generation unit. The symmetric key generation unit produces an ephemeral asymmetric key pair including an ephemeral asymmetric public key and an ephemeral asymmetric private key.

WO 02/060121 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A PLATFORM AND METHOD FOR SECURELY TRANSMITTING AUTHORIZATION DATA

BACKGROUND

1. Field

This invention relates to the field of data security. In particular, the invention relates to a platform and method for securely transmitting information using an ephemeral asymmetric key pair.

2. Background

In today's society, it is becoming necessary to transmit digital data from one location to another in a manner that is clear and unambiguous to a legitimate receiver, but incomprehensible to any illegitimate recipients. Accordingly, such data is typically encrypted by a software application executing some predetermined encryption algorithm and is transmitted to the legitimate receiver in encrypted form. The legitimate receiver then decrypts the transmitted data for use.

Often, encryption/decryption of data is accomplished through symmetric key cryptography. For symmetric key cryptography, the sender uses a key to encrypt data prior to transmission over an unsecured link. The receiver uses the same key to decrypt the data upon receipt. Although symmetric key cryptography is computationally simple, it requires complex key management. For instance, each sender would require a different symmetric key to communicate with an intended receiver, thereby making it difficult, if not impossible, to support a large number of persons. Another method of encryption/decryption is to create two separate keys (referred to as a "key pair"). One key (public key) of the key pair is normally used for encryption while the other key (private key) of the key pair is normally used for decryption of the data. This method is commonly referred to as "asymmetric key cryptography". One disadvantage associated with asymmetric key cryptography is that the key pairs are not erasable after each communication session. Instead, they are permanently assigned and used for all communications. Thus, any disclosure of the private key mitigates or perhaps eliminates the security of any subsequent or previous communications.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an exemplary embodiment of a platform practicing the invention.

Figure 2 is an exemplary embodiment of the IC device as a Trusted Platform Module (TPM) employed within the platform of Figure 1.

Figure 3 is an exemplary embodiment of a flowchart illustrating the secure data transmission mechanism.

Figure 4 is an exemplary embodiment of a block diagram for verifying that an ephemeral asymmetric public key (EAPUK) is a valid key through validation of the ephemeral credential and the EAPUK without using hash operation(s).

Figure 5 is an exemplary embodiment of a block diagram for verifying that EAPUK is a valid key through validation of the ephemeral credential and the EAPUK using hash operation(s).

DESCRIPTION

The present invention relates to a platform and method for securely transmitting information such as authorization secret for example. Once loaded within a device, the authorization secret uses cryptographic operations to validate authorization data that accompanies an operation request directed to the device. In the event that the authorization data is validated, the device performs the requested operation. The secure transmissions may be accomplished through utilization of ephemeral asymmetric key pair(s) as described below.

In the following description, certain terminology is used to describe various features of the present invention. For example, a "platform" includes any product including a device (e.g., one or more packaged or unpackaged integrated circuits) that processes data. Examples of various types of platforms include, but are not limited or restricted to a computer (e.g., desktop, laptop, server, workstation, personal digital assistant, etc.) or any peripheral associated therewith, wireless communication device (e.g., telephone handset, pager, etc.), a television set-top box and the like. A "link" is broadly defined as a logical or physical communication path such as, for instance, electrical wire, optical fiber, cable, bus

trace, or even a wireless channel using infrared, radio frequency (RF), or any other wireless signaling mechanism.

In addition, the terms "information" or "content" are defined as one or more bits of data, address, control or any combination thereof. "Code" includes software or firmware that, when executed, performs certain functions. Examples of different types of code include an application, an applet, or any series of instructions.

Herein, various cryptographic terms are used to describe other features of the invention. For example, an "entity" is information used by a device to perform operations. For instance, an entity could be an asymmetric key, a symmetric key or random data. Entities temporarily held in locations outside an internal memory of the device are normally encrypted. When an entity is loaded into an internal memory of a device, an authorization secret for the entity is also loaded. The "authorization secret" is information held by the device (e.g., in its internal memory). Knowledge of the authorization secret allows access to the entity, and/or information stored in the internal memory, and/or allows certain operations to be performed by the platform implemented with the device.

"Authorization data" is the result of a cryptographic operation that proves knowledge of the authorization secret for an entity and should accompany each operation request.

An "identity" is a specific type of entity. For one embodiment, an identity includes a label that is unique within some context and attached to an object (e.g., segments of executable code) and/or secret data that is statistically improbable to estimate without disclosure. For instance, with respect to this embodiment, the secret data may include a permanent asymmetric key pair as described below. This allows a platform to support different access privileges to stored content or different operations, depending on the identity conferred by the requester. To prove an identity, a cryptographic engine operates on input data, using the secret data, to produce output data where the output data is statistically impossible to produce without the secret data. The capability of producing the output data is taken as proof of possession of the secret data, and hence as proof of identity.

It is appreciated that certain details are set forth in order to provide a thorough understanding of the present invention. It will be apparent to a person of ordinary skill in the art, however, that the present invention may be practiced through many embodiments

other that those illustrated. Well-known circuits are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

Referring to Figure 1, an exemplary block diagram of an illustrative embodiment of a platform 100 employing the present invention is shown. The platform 100 comprises a processor 110, a memory control hub (MCH) 120, a system memory 130, an input/output control hub (ICH) 140, and an integrated circuit (IC) device 150 which initiates, monitors and controls the authentication process of the platform 100.

As shown in Figure 1, the processor 110 represents a central processing unit of any type of architecture, such as complex instruction set computers (CISC), reduced instruction set computers (RISC), very long instruction word (VLIW), or a hybrid architecture. In one embodiment, the processor 110 is compatible with the INTEL® Architecture (IA) processor, such as the IA-32 and the IA-64. Of course, in an alternative embodiment, the processor 110 may include multiple processing units coupled together over a common host bus 105.

Coupled to the processor 110 via the host bus 105, the MCH 120 may be integrated into a chipset that provides control and configuration of memory and input/output devices such as the system memory 130 and the ICH 140. The system memory 130 stores system code and data. The system memory 130 is typically implemented with dynamic random access memory (DRAM) or static random access memory (SRAM).

The ICH 140 may also be integrated into a chipset together or separate from the MCH 120 to perform I/O functions. As shown, the ICH 140 supports communications with the IC device 150 via link 160. Also, the ICH 140 supports communications with components coupled to other links such as a Peripheral Component Interconnect (PCI) bus at any selected frequency (e.g., 66 megahertz "MHz", 100 MHz, etc.), an Industry Standard Architecture (ISA) bus, a Universal Serial Bus (USB), a Firmware Hub bus, or any other bus configured with a different architecture than those briefly mentioned. The ICH 140 may be coupled to non-volatile memory 170 (e.g., flash memory) that contains Basic Input/Output System (BIOS) code for example.

Referring to Figure 2, an exemplary embodiment of the IC device 150 is shown as a Trusted Platform Module (TPM), which features one or more integrated circuits placed within a protective package 200. For instance, the protective package 200 may be any type of IC package such as an IC package for a single IC or a package for a multi-chip

module. Alternatively, the protective package 200 may include a cartridge or casing covering a removable daughter card featuring the integrated circuit(s) and the like.

As shown in Figure 2, the TPM 150 comprises an input/output (I/O) interface 210, a processor 220, internal memory 230 (e.g., volatile and/or non-volatile), an asymmetric key generation unit 240 and a cryptographic engine 250. It is contemplated that the cryptographic engine 250 may be part of the processor 220 or separate logic therefrom.

Herein, the asymmetric key generation unit 240 is configured to create one or more (N) ephemeral asymmetric key pairs 260_1-260_N. Each key pair 260_1-260_N includes an ephemeral asymmetric private key (EAPRK) 261_1-261_N and a corresponding ephemeral asymmetric public key (EAPUK) 262_1-262_N. Each ephemeral asymmetric key pair 260_1-260_N is used for encryption and decryption operations during a single communication session with another platform and may be erased after completion of the communication session either automatically or through issuance of an authenticated software command. For instance, a single communication session may involve (i) establishment of communications with another platform, (ii) creation of a new entity (including the transmission of authorization data) and (iii) termination of the communications.

The TPM 150 allows access to certain entities stored in a portion of the internal memory 230 and/or performance of selected operations by its platform only upon receipt of authorization data by the processor 220.

In order to protect the confidentiality of an authorization secret during transmission to the TPM 150 as well as insure its integrity, the TPM 150 utilizes a secure data transmission mechanism. The confidentiality of transmissions is protected through encryption of the authorization secret. Likewise, its integrity is protected by the ability of the sender to verify that the authorization secret is being transferred to a TPM and that only a specific TPM can decrypt the data.

Referring to Figure 3, an exemplary embodiment of a flowchart illustrating the secure data transmission mechanism is shown. Initially, the platform is loaded with an identity and a credential associated with that identity (block 300). The "identity credential" may include (i) secret data associated with the identity (e.g., a permanent asymmetric public key of the identity, referred to as the "identity public key") and (ii) a first sequence of alphanumeric characters (e.g., a statement "TCPA Subsystem Identity"). This information is digitally signed with a private key (CAPRK) of a certification authority being a trusted third party such as an original equipment manufacturer, a

governmental agency, a bank, a designated certification entity and the like. Of course, prior to the digitally signing operation, the at least a portion of the secret data and the first sequence of alphanumeric characters may collectively undergo a hash operation.

In order to create a new entity for the platform, the requester initiates an entity creation request that specifies which identity that the requester wishes to use for validation purposes (block 305). For instance, the platform may employ multiple software tools that constitute identities, each having a unique name (or label). In response to receiving the entity creation request, the TPM generates an ephemeral asymmetric key pair for the new TPM entity (block 310). The ephemeral asymmetric key pair includes an ephemeral asymmetric public key (EAPUK) and an ephemeral asymmetric private key (EAPRK).

Thereafter, as described in block 315, the EAPUK is certified internally within the TPM (e.g., digital certification performed by the cryptographic engine 250 of Figure 2 using a portion of the secret data associated with the selected identity). This produces an ephemeral credential. Normally, the "ephemeral credential" includes the EAPUK and a second sequence of alphanumeric characters (e.g., a statement "TCPA Trusted Platform Module Endorsement"), both can be digitally signed with a portion of the secret data such as a private key associated with the identity (referred to as the "identity private key"). Of course, prior to the digitally signing operation, the EAPUK and the second sequence of alphanumeric characters may collectively undergo a hash operation.

In another embodiment, the ephemeral credential includes the EAPUK, the second sequence of alphanumeric characters and an identity label. This information in its entirety may be digitally signed with the identity private key, or in the alternative, this information may undergo successive or reiterative hash operations to produce a hash value, where the hash value is digitally signed with the identity private key. In yet another embodiment, the ephemeral credential may be the EAPUK digitally signed with the identity private key.

Thereafter, the EAPUK, ephemeral credential, secret data associated with the identity (e.g., at least the identity public key) and the identity credential are transmitted over a link to the requester (block 320). The requester can validate the identity using the identity credential by gaining access to a widely disseminated public key (CAPUK) of the certification authority (block 325). The requester then validates the EAPUK and the ephemeral credential as being signed by the identity private key since the identity credential features the identity public key (block 330). This allows the requester to now believe that the EAPUK came from a valid TPM without knowledge of which particular

TPM. Also, this allows the requester to have confidence that only a TPM will be able to decrypt an authorization secret.

In the situation where the digital signing operation does not utilizing a hash operation, as shown in Figure 4, the ephemeral credential and EAPUK are validated by recovering the identity public key from the identity credential (block 400). This is due to the fact that the public key of the certification authority may be readily available. Upon recovery of the identity public key, the ephemeral asymmetric public key can be recovered from the ephemeral credential (block 410). The recovered ephemeral asymmetric public key is then compared with EAPUK (block 420). If both values compare, the EAPUK is valid and properly certified (block 430). Otherwise, EAPUK is not certified (block 440).

Alternatively, in the situation where the digital signing operation utilizes a hash operation, the ephemeral credential and EAPUK are validated by recovering the identity public key from the identity credential (block 500). Upon recovery of the identity public key, a hash value of the ephemeral credential can be recovered from the ephemeral credential (block 510). Moreover, a hash operation is performed on the EAPUK (and perhaps the second sequence of alphanumeric characters or identity label if applicable) to produce a hash result (block 520). The hash result is then compared to the hash value (block 530). If the hash result matches the hash value, the EAPUK is valid and properly certified (block 540). Otherwise, EAPUK is not certified (block 550).

Referring back to Figure 3, the authorization secret is encrypted using EAPUK (block 335). In one embodiment, the size of the authorization secret is set at M bits (e.g., $M \leq 160$ bits) so the asymmetric cryptographic function is able to encrypt the authorization secret. Also, the authorization secret may contain some static markers to allow the TPM to determine if decryption was successful.

The encrypted authorization secret is transmitted over a link to the TPM along with static markers and perhaps additional parameters necessary for creation of the entity (block 340). Upon receipt, the TPM decrypts the encrypted authorization secret using EAPRK and determines whether the decryption was successful through comparison of static markers for example (block 345). If the decryption was successful, the decrypted authorization secret is used as the authorization secret for the new TPM entity (block 350). Otherwise, an error is reported (block 355).

While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely

illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art. Additionally, it is possible to implement the present invention or some of its features in hardware, firmware, software or a combination thereof where the software is provided in a processor readable storage medium such as a magnetic, optical, or semiconductor storage medium.

CLAIMS

What is claimed is:

1. A method comprising:

receiving an ephemeral asymmetric public key and an ephemeral credential;

verifying that the ephemeral asymmetric public key is valid using data recovered from the ephemeral credential;

encrypting authorization secret using the ephemeral asymmetric public key if the ephemeral asymmetric public key is determined to be valid; and

transmitting the encrypted authorization secret over a link.

2. The method of claim 1, wherein the ephemeral credential includes at least a duplicate copy of the ephemeral asymmetric public key digitally signed with an identity private key.

3. The method of claim 2, wherein prior to verifying that the ephemeral asymmetric public key is valid, the method further comprises receiving of an identity public key and an identity credential.

4. The method of claim 3, wherein the ephemeral credential further includes a predetermined sequence of alphanumeric characters.

5. The method of claim 2, wherein the verifying that the ephemeral asymmetric public key is valid includes

recovering the duplicate copy of the ephemeral asymmetric public key from the ephemeral credential; and

comparing the duplicate copy of the ephemeral asymmetric public key with the ephemeral asymmetric public key.

6. The method of claim 5, wherein the recovering of the duplicate copy of the ephemeral asymmetric public key includes decrypting the ephemeral credential with an identity public key.

7. The method of claim 1, wherein the link routes the encrypted authorization secret to a trusted platform module including an input/output interface, a processor, an internal memory and an asymmetric key generation unit.

8. The method of claim 7 further comprising:

recovering the authorization secret by decrypting the encrypted authorization secret using an ephemeral asymmetric private key corresponding to the ephemeral asymmetric public key, both the ephemeral asymmetric private key and the ephemeral asymmetric public key are temporarily used for a single communication session.

9. The method of claim 8, wherein prior to receiving the ephemeral asymmetric public key and the ephemeral credential, both the ephemeral asymmetric public key and the ephemeral asymmetric private key are created by the asymmetric key generation unit within the trusted platform module.

10. A method comprising:

creating an ephemeral asymmetric public key and a corresponding ephemeral asymmetric private key internally within an integrated circuit device;

certifying the ephemeral asymmetric public key;

transmitting the ephemeral asymmetric public key and an ephemeral credential to an requester in order to determine whether the ephemeral asymmetric public key is valid; and

using the ephemeral asymmetric public key for protecting confidentiality of an authorization secret provided by the requester during a communication session.

11. The method of claim 10, wherein the authorization secret is any type of information that enables access to stored content within the integrated circuit device.

12. The method of claim 10, wherein the authorization secret is any type of information that enables selected functionality for a platform including the integrated circuit device.

13. The method of claim 10, wherein protecting of the confidentiality of the authorization data includes encrypting the authorization secret using the ephemeral asymmetric public key.

14. An integrated circuit device comprising:

an internal memory; and

an asymmetric key generation unit to produce an ephemeral asymmetric key pair including an ephemeral asymmetric public key and an ephemeral asymmetric private key, both the ephemeral asymmetric public key and the ephemeral asymmetric private key are temporarily used for encryption and decryption during a single communication session.

15. The integrated circuit device of claim 14, wherein the internal memory contains the ephemeral asymmetric key pair and an asymmetric key cryptography function for execution by the asymmetric key generation unit.

16. The integrated circuit device of claim 14 further comprising an integrated circuit package encapsulating the internal memory and the asymmetric key generation unit.

17. The integrated circuit device of claim 16 further comprising:

a processor coupled to the internal memory and contained within the integrated circuit package; and

an input/output (I/O) interface coupled to the processor.

18. A platform comprising:

a processor;

an input/output control hub; and

a trusted platform module (TPM) coupled to the input/output control hub, the TPM including

an internal memory, and

an asymmetric key generation unit to produce an ephemeral asymmetric key pair including an ephemeral asymmetric public key and an ephemeral asymmetric

private key, both the ephemeral asymmetric public key and the ephemeral asymmetric private key are temporarily used for encryption and decryption during a single communication session.

19. The platform of claim 18, wherein the internal memory of the TPM contains the ephemeral asymmetric key pair and an asymmetric key cryptography function for execution by the asymmetric key generation unit.

20. The platform of claim 18, wherein the TPM further comprises an integrated circuit package including the internal memory and the asymmetric key generation unit.

21. The platform of claim 20, wherein the TPM further comprises

a processor coupled to the internal memory and contained within the integrated circuit package; and

an input/output (I/O) interface coupled to the processor.

22. A program loaded into readable memory for execution by a trusted platform module of a platform, the program comprising:

code to receive an ephemeral asymmetric public key and an ephemeral credential;

code to verify that the ephemeral asymmetric public key is valid using data recovered from the ephemeral credential;

code to encrypt an authorization secret using the ephemeral asymmetric public key if the ephemeral asymmetric public key is determined to be valid, the authorization secret to control access to an entity loaded on the platform; and

code to transmit the encrypted authorization secret over a link to the platform.

23. The program of claim 22, wherein the ephemeral credential includes at least a duplicate copy of the ephemeral asymmetric public key digitally signed within with trusted platform module.

24. The program of claim 22, wherein the credential further includes a predetermined sequence of alphanumeric characters to indicate that the ephemeral asymmetric public key originated from a selected identity of the trusted platform module.

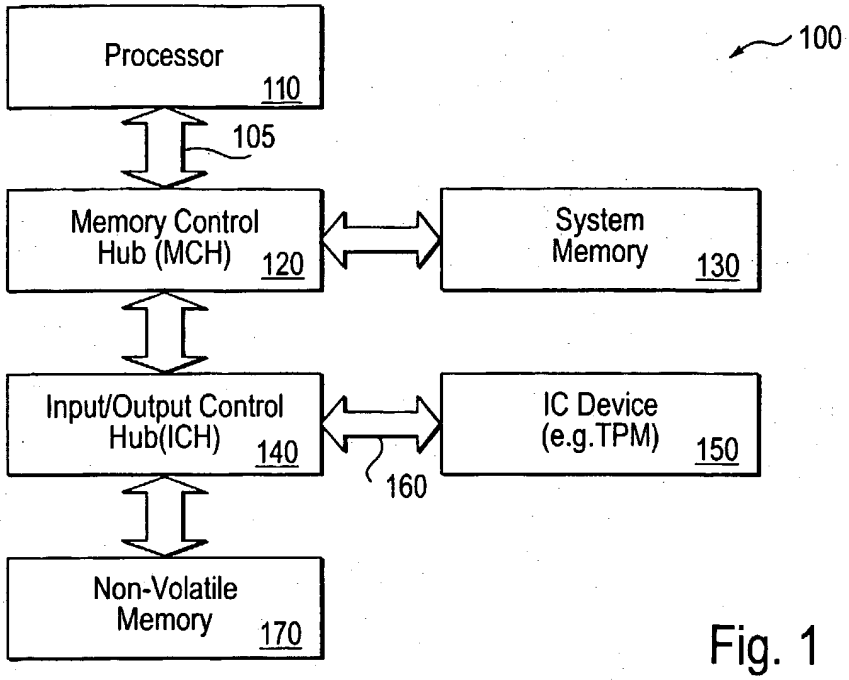

Processor
110
100
105
Memory Control
Hub (MCH)
120
System
Memory
130
Input/Output Control
Hub(ICH)
140
IC Device
(e.g.TPM)
150
160
Non-Volatile
Memory
170

Fig. 1

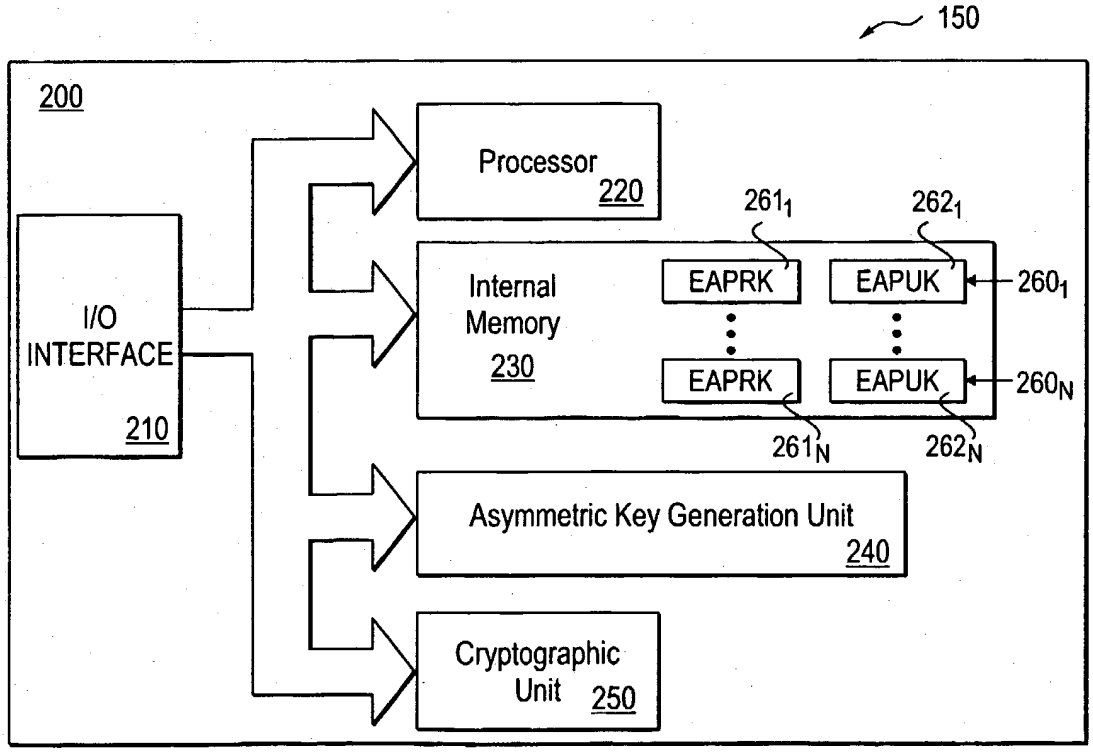

150
200
Processor
220
261_1
262_1
I/O
INTERFACE
210
Internal
Memory
230
EAPRK
EAPUK
260_1
EAPRK
EAPUK
260_N
261_N
262_N
Asymmetric Key Generation Unit
240
Cryptographic
Unit
250

Fig. 2

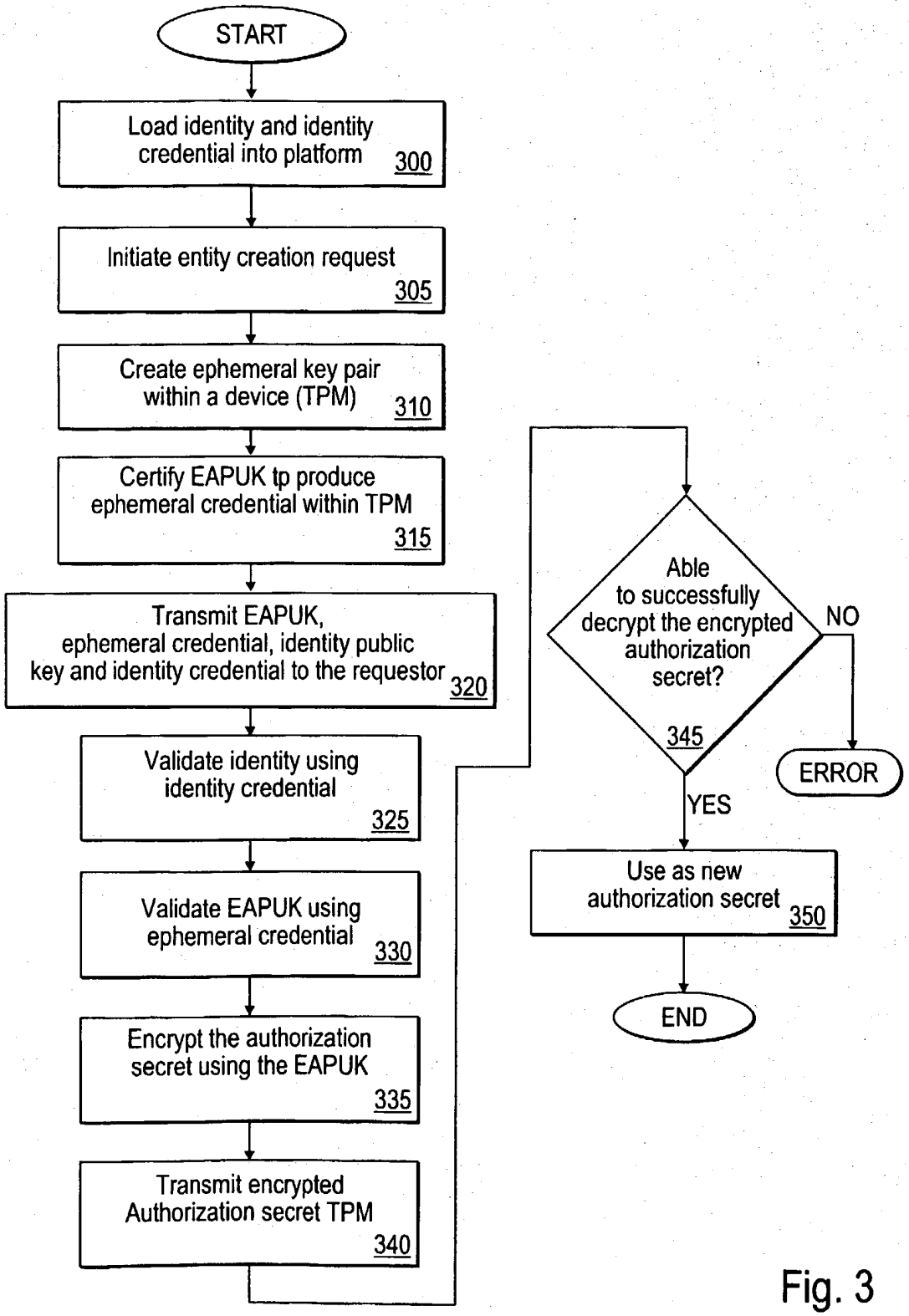

START
Load identity and identity credential into platform 300
Initiate entity creation request 305
Create ephemeral key pair within a device (TPM) 310
Certify EAPUK tp produce ephemeral credential within TPM 315
Transmit EAPUK, ephemeral credential, identity public key and identity credential to the requestor 320
Validate identity using identity credential 325
Validate EAPUK using ephemeral credential 330
Encrypt the authorization secret using the EAPUK 335
Transmit encrypted Authorization secret TPM 340
Able to successfully decrypt the encrypted authorization secret? 345
NO
ERROR
YES
Use as new authorization secret 350
END

Fig. 3

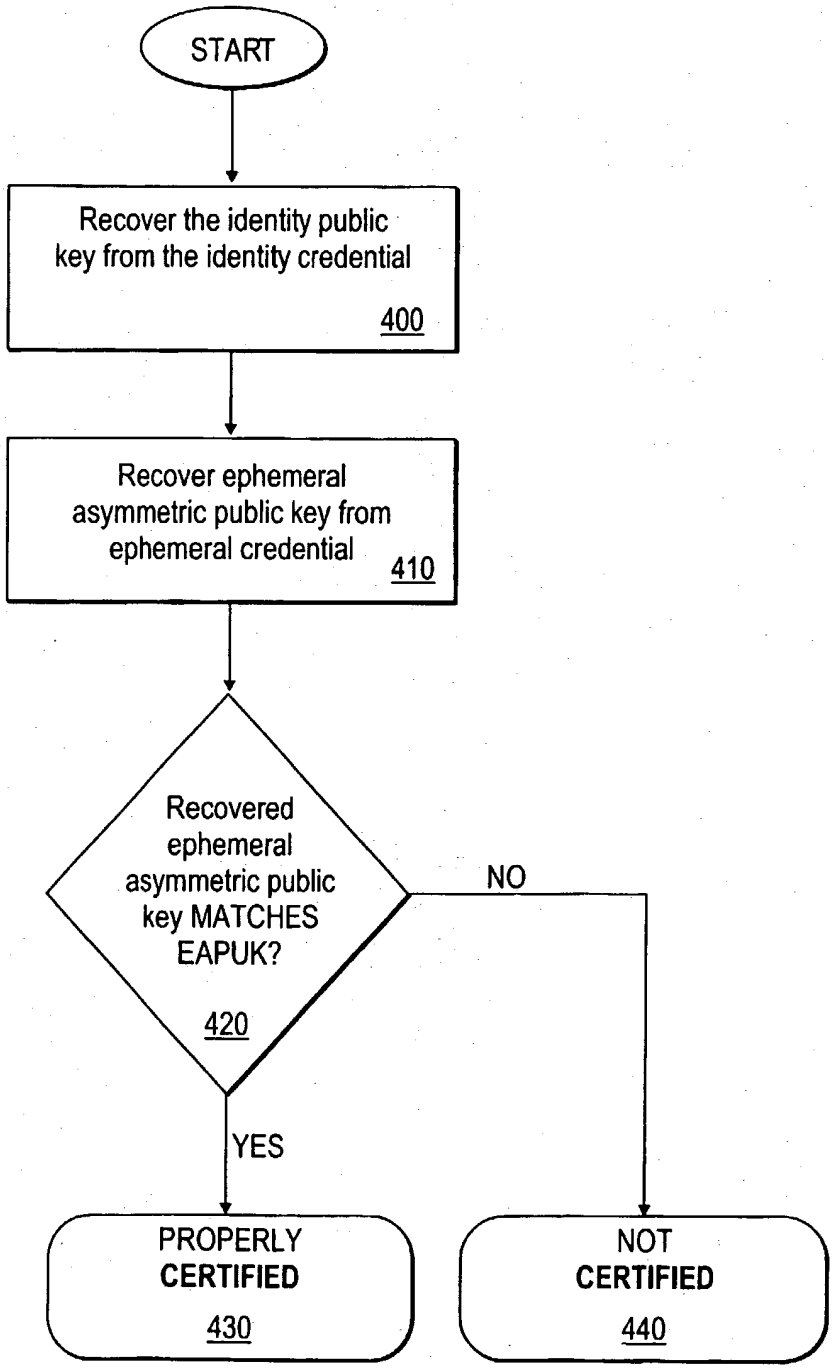

START
Recover the identity public key from the identity credential
400
Recover ephemeral asymmetric public key from ephemeral credential
410
Recovered ephemeral asymmetric public key MATCHES EAPUK?
420
NO
YES
PROPERLY CERTIFIED
430
NOT CERTIFIED
440

Fig. 4

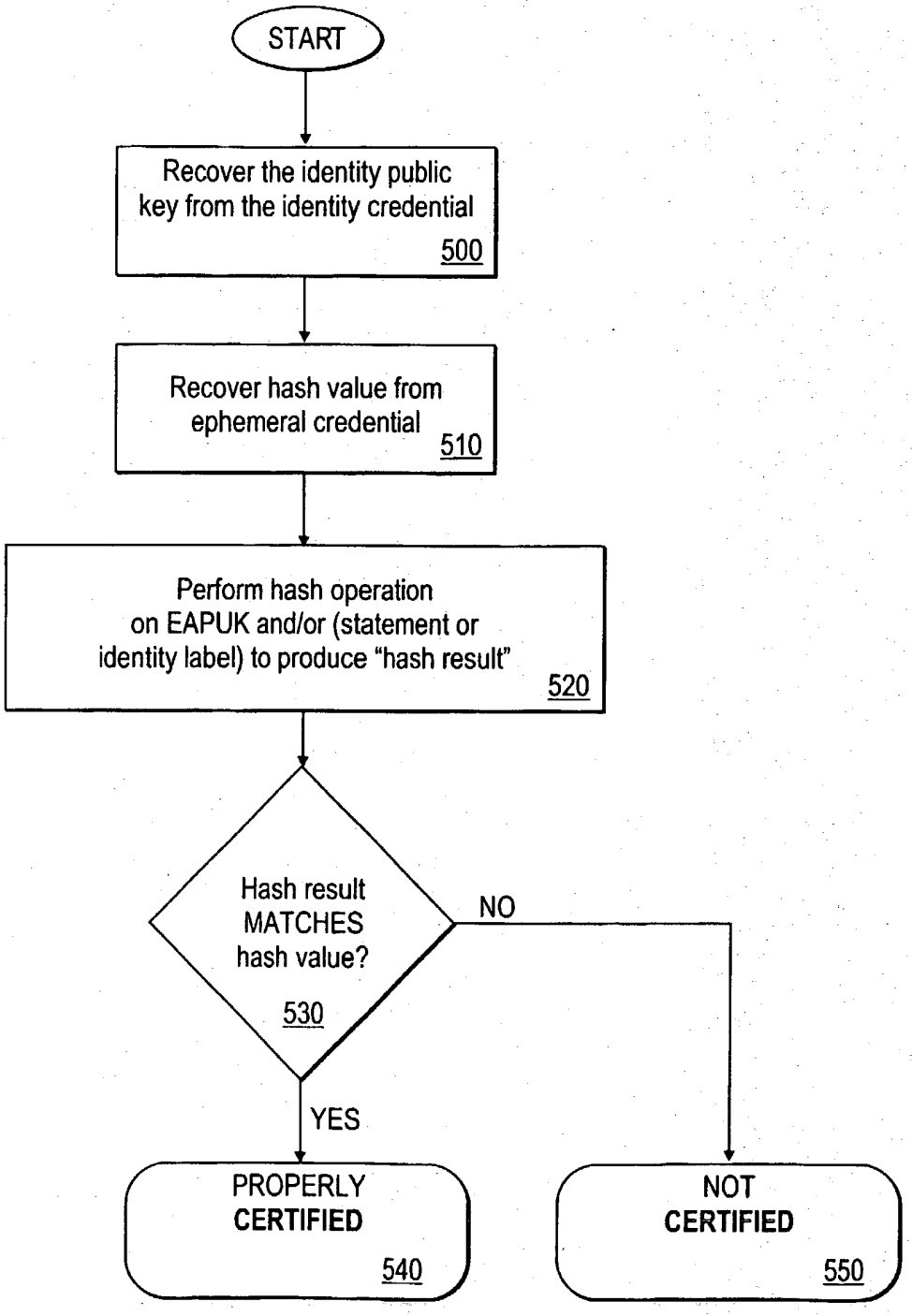

START
Recover the identity public key from the identity credential
500
Recover hash value from ephemeral credential
510
Perform hash operation on EAPUK and/or (statement or identity label) to produce "hash result"
520
Hash result MATCHES hash value?
530
NO
YES
PROPERLY CERTIFIED
540
NOT CERTIFIED
550

Fig. 5

INTERNATIONAL SEARCH REPORT

PCT/US 01/43736

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 05837 A (CERTICOM CORP ;VADEKAR ASHOK (CA); LAMBERT ROBERT J (CA)) 3 February 2000 (2000-02-03) page 4 ---	1-24
X	LINN J: "Practical authentication for distributed computing" PROCEEDINGS OF THE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY. OAKLAND, MAY 7 - 9, 1990, LOS ALAMITOS, IEEE COMP. SOC. PRESS, US, vol. SYMP. 11, 7 May 1990 (1990-05-07), pages 31-40, XP010020184 ISBN: 0-8186-2060-9 * Chapter 2.3.2 * --- -/--	1-24

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 June 2002	08/07/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	San Millán Maeso, J

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	MENEZES, OORSCHOT: "Handbook of Applied Cryptography" 1997 , CRC PRESS LLC , USA XP002202168 page 559 -page 560 -----	1-24

INTERNATIONAL SEARCH REPORT

PCT/US 01/43736

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0005837 A	03-02-2000	AU 4891799 A	14-02-2000
		WO 0005837 A1	03-02-2000
		EP 1097541 A1	09-05-2001
		US 2001033655 A1	25-10-2001